STATE OF NEVADA

GAMING CONTROL BOARD

MINIMUM INTERNAL CONTROL STANDARDS

Note: When adopted in 1997, these standards applied to both Group I and Group II licensees. In February 2000, the Nevada Gaming Commission amended the definition of "Group II licensee" and revised Regulation 6.090 to require that Group II licensees (i.e., redefined as those licensees with annual gross gaming revenues of less than $3 million) follow Internal Control Procedures rather than the Minimum Internal Control Standards. Therefore, although these standards make numerous references to Group II licensees, these standards no longer apply to such licensees – they only apply to those licensees with annual gross gaming revenues of $3 million or more. References to Group II licensees will be deleted with the next formal revision of the Minimum Internal Control Standards.

ELECTRONIC DATA PROCESSING

General Controls

Standards 1 through 6 should be addressed in the system of internal control for each applicable gaming section.

1. The main computers (i.e., hardware, software and data files) for each gaming application (e.g., keno, race and sports, slots, etc.) and each casino entertainment application are in a secured area with access restricted to authorized persons, including vendors.

2. Gaming and food/beverage personnel are precluded from having unrestricted access to the secured computer areas.

3. The computer systems, including application software, are secured through the use of passwords or other approved means. Management personnel or persons independent of the department being controlled will assign and control access to system functions.

4. Passwords are controlled as follows unless otherwise addressed in these standards:

    a. Each user must have their own individual password.

    b. Passwords are changed at least quarterly with changes documented.

5. Adequate backup and recovery procedures are in place, and if applicable, include:

    a. Daily backup of data files.

    b. Backup of all programs.

    c. Secured off-site storage of all backup data files and programs, or other adequate protection.

    d. Recovery procedures are tested at least annually.

6. Adequate system documentation is maintained, including descriptions of both hardware and software, operator manuals, etc.

EDP Department

If a separate EDP department is maintained or if there are in-house developed systems, Standards 7 through 10 are applicable.

7. The EDP department is independent of the gaming areas (e.g., cage, pit, count rooms, etc.).

ELECTRONIC DATA PROCESSING

8. EDP department personnel are precluded from unauthorized access to:

    a. Computers and terminals located in gaming areas.

    b. Source documents.

    c. Live data files (not test data).

9. Program changes for in-house developed systems are documented as follows:

    a. Requests for new programs or program changes are reviewed by the EDP supervisor. Approvals to begin work on the program are documented.

    b. A written plan of implementation for new and modified programs is maintained and includes, at a minimum, the date the program is to be placed into service, the nature of the change (if applicable), a description of procedures required in order to bring the new or modified program into service (conversion or input of data, installation procedures, etc.), and an indication of who is to perform all such procedures.

    c. Testing of new and modified programs is performed and documented prior to implementation.

    d. A record of the final program or program changes, including evidence of user acceptance, date in service, programmer, and reason for changes, is documented and maintained.

10. Computer security logs, if generated by the system, are reviewed by EDP supervisory personnel for evidence of:

    a. Multiple attempts to log-on. Alternatively, the system will deny user access after three attempts to log-on.

    b. Changes to live data files.

    c. Any other unusual transactions.

    Note: This standard does not apply to personal computers.

Modems

11. If remote dial-up to any associated equipment is allowed for software support, the licensee must maintain an access log which includes: name of employee authorizing modem access, name of authorized programmer or manufacturer representative, reason for modem access, description of work performed, date, time, and duration of access.

ELECTRONIC DATA PROCESSING

Optical Disk Document Storage

12. Documents may be scanned or directly stored to WORM ("Write Once Read Many") optical disk with the following conditions:

    a. The optical disk must contain the exact duplicate of the original document.

    b. All documents stored on optical disk must be maintained with a detailed index containing the casino department and date in accordance with Regulation 6.040(1). This index must be available upon Board request.

    c. Upon request by Board agents, hardware (terminal, printer, etc.) must be provided in order to perform auditing procedures.

    d. Controls must exist to ensure the accurate reproduction of records, up to and including the printing of stored documents used for auditing purposes.

13. If source documents and summary reports are stored on re-writeable optical disks, the disks may not be relied upon for the performance of any audit procedures, and the original documents and summary reports must be retained.